

REMARKS

In the final Office Action¹, the Examiner rejected claims 1-5, 13-15, 20-24, 32-36, 44-46, and 51-55 under 35 U.S.C. § 103(a) as unpatentable over JP 10-65662 to Ishiguro et al. ("*Ishiguro*"); U.S. Patent No. 6,314,409 to Schneck et al. ("*Schneck*"); U.S. Patent No. 6,374,036 to Ryan et al. ("*Ryan*"); and "Applied Cryptography" by Schnier ("*Schnier*").

By this Amendment, Applicants amend claims 1-5, 13-15, 20-24, 32-36, 44-46, and 51-55. Claims 1-5, 13-15, 20-24, 32-36, 44-46, and 51-55 remain pending and under current examination.

Applicants respectfully traverse the rejection of claims 1-5, 13-15, 20-24, 32-36, 44-46, and 51-55 under 35 U.S.C. § 103(a).

Independent claim 1, for example, recites an information-signal playback system comprising an information-signal reading apparatus and an information-signal processing apparatus, the information-signal processing apparatus comprising, among other things, a "storage means for storing the encrypted identification information and the identification information." The four cited references, even if combined as suggested by the Examiner, fail to teach or suggest the claimed storage means.

¹ As Applicants' remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicants' silence as to certain requirements applicable to such rejections (e.g., whether a reference constitutes prior art, motivation to combine references) is not a concession by Applicants that such requirements have been met, and Applicants reserve the right to analyze and dispute such in the future.

The Examiner concedes that *Ishiguro* fails to disclose an output means for supplying both encrypted and unencrypted information on copyright protection (final Office Action at p. 4). *Ishiguro* also fails to disclose a “storage means for storing the encrypted identification information and the identification information” as recited by independent claim 1.

Schneck also fails to disclose the claimed storage means. *Schneck* discloses distributing packaged data 108 that includes an encrypted version of access rules 116 (*Schneck*, col. 10, lines 47-53, and Fig. 2). Alternately, *Schneck* discloses that access rules 116 can be provided separately from packaged data 108 (*Schneck*, col. 10, line 49). Thus, *Schneck* uses one of two secure methods for ensuring the secrecy of access rules 116, either encrypting them, or providing them separately to a trusted user. However, the access rules in *Schneck* are not “identification information.” Moreover, *Schneck* does not disclose storing both an encrypted and an unencrypted copy of access rules 116 in a storage medium. *Schneck*, therefore, does not teach or suggest the claimed “storage means for storing the encrypted identification information and the identification information” as recited by independent claim 1.

Ryan also fails to disclose the claimed storage means. *Ryan* discloses, “a watermark . . . is conventionally embedded in a video image. A subset of the watermark bits carries a digital attribute (a number) which is a numeric characteristic of the video signal, for instance an average amplitude of the video signal over one video field or frame (*Ryan* col. 3, lines 1-6). *Ryan* continues, “[t]he compliant digital video

recorder . . . examines the watermark, verifies it, . . . and extracts the associated attribute value from the watermark. The compliant recorder also . . . measures the attribute of that particular field, and compares the measured attribute to the extracted attribute value" (*Ryan* col. 3, lines 26-36). However, the attribute value in *Ryan* is not "identification information." Moreover, *Ryan* does not disclose storing the attribute value in both an encrypted and unencrypted form in the video image, but rather the "compliant recorder" measures or calculates the attribute value from the video image itself. Thus, *Ryan* does not teach or suggest the claimed "storage means for storing the encrypted identification information and the identification information" as recited by independent claim 1.

Schnier also fails to disclose the claimed storage means. *Schnier* discloses a "one-way hash function . . . that takes a variable-length input (called a pre-image) and converts it to a fixed-length (generally smaller) output string (called a hash value)" (*Schnier* p. 30). First, the hash function disclosed by *Schnier* does not correspond to the claimed "encryption," as *Schnier* discloses "[t]he hash function is public; there's no secrecy to the process" (*Schnier* p. 30). Moreover, *Schnier* makes no mention of storing both the hash value and the pre-image in a storage means. *Schnier* therefore fails to teach or suggest the claimed "storage means for storing the encrypted identification information and the identification information" as recited by independent claim 1.

Further, Applicants disagree with the Examiner's assertion that *Schnier* teaches the claimed comparing means (Final Office Action at p. 5). The claimed comparing means is "for comparing the decrypted identification information with the identification information to judge if an attempt to alter the identification information has been performed."

Schnier discloses applying a hash function to two data items, and comparing the results to determine if the data items are identical. (*Schnier* p. 31). However, the hash functions disclosed by *Schnier* are not a form of encryption. The term "encrypt" is understood as a conversion of a "plaintext" version of data into an encrypted version of the data, so that the plaintext can only be recovered from the encrypted version by an authorized party. In contrast, when *Schnier's* hash function is applied to data, the plaintext version of the data cannot be recovered. *Schnier* discloses as much, indicating at p. 31 that "it is computationally unfeasible to find a pre-image that hashes to a given value." Therefore, *Schnier's* hash functions are not the same as encryption functions, and *Schnier's* teaching of comparing hash values is not the same as comparing decrypted information with unencrypted information. Therefore, *Schnier* fails to teach the claimed comparing means. The remaining references also fail to disclose the claimed comparing means.

Although of different scope, independent claims 13, 20, 32, 44 and 51 distinguish over the four cited references for at least the same reasons as claim 1. Claims 2-5 depend from claim 1; claims 14 and 15 depend from claim 13; claims 21-24 depend

from claim 20; claims 33-36 depend from claim 32; claims 45 and 46 depend from claim 44; and claims 52-55 depend from claim 51. As already discussed, the cited references fail to teach or suggest the claimed output means and comparing means.

As discussed in the Reply to Office Action filed September 29, 2006, dependent claim 2 recites additional features not taught by the cited references. While the Examiner provides a "Response to Arguments" section in the final Office Action, the Examiner has not addressed Applicants' reasoning regarding claim 2 (final Office Action, pages 2-3). Instead, the Examiner merely duplicates the language used in the previous Office Action (Office Action mailed August 15, 2006 at p. 4, final Office Action at pp. 5-6).

Dependent claim 2 recites the information-signal reading apparatus of claim 1, "wherein the identification information is media-type information," and claim 1 recites "comparing the decrypted identification information with the identification information." The cited references fail to teach or suggest "comparing the decrypted identification information with the identification information" wherein the "identification information is media-type information indicating the type of the recording medium" as required by claim 2.

The Examiner cites to portions of *Schneck* and *Ryan* that allegedly disclose "media-type information indicating the type of the recording medium" (final Office Action at p. 4). However, neither of these references discloses any comparison of the media-

type information. Moreover, neither of these references discloses encrypted or decrypted media-type information.

Schneck merely discloses, "in a video cassette recorder ... a single control program may be running at all times ... all access to controlled data is initiated by the control program" (*Schneck* col. 18, lines 11-16). The controlled data is not "media-type information." The controlled data does not indicate the type of recording medium. *Schneck* does not disclose comparing the controlled data with any other data that could reasonably be considered "media-type information." *Schneck* does not disclose encrypted or decrypted controlled data. *Schneck* therefore fails to teach or suggest the claimed "comparing the decrypted identification information with the identification information" wherein the "identification information is media-type information indicating the type of the recording medium" as required by claim 2.

Ryan also fails to disclose this subject matter of claim 2. The cited portions of *Ryan* disclose a copy-once method for digital recording that requires only one watermark (*Ryan*, col. 2, lines 29-34). The watermark in *Ryan* is not "media-type information." The watermark does not indicate the type of recording medium. *Ryan* does not disclose comparing an unencrypted watermark with an encrypted watermark. *Ryan* therefore fails to teach or suggest the claimed "comparing the decrypted identification information with the identification information" wherein the "identification information is media-type information indicating the type of the recording medium" as required by claim 2.

Because the cited references fail to teach or suggest each and every claim element recited by claims 1-5, 13-15, 20-24, 32-36, 44-46, and 51-55, no prima facie case of obviousness has been established with respect to these claims. Applicants therefore request the Examiner to withdraw the rejection of these claims under 35 U.S.C. § 103(a).

In view of the foregoing remarks, Applicants respectfully request reconsideration of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

Dated: May 11, 2007

By: 

Michael R. Kelly
Reg. No. 33,921